CLAIMS

1. An encryption method, comprising the steps of:

dividing a plaintext to be encrypted thereby to obtain a plaintext vector;

applying a predetermined transformation on the plaintext vector thereby to generate a transformation vector; and

generating a ciphertext by a product-sum operation between the components of a public key vector and the components of the plaintext vector and the transformation vector.

2. The encryption method of Claim 1, wherein

the product-sum operation with the components of the public key vector is performed using alternately a component of the plaintext vector and a component of the transformation vector.

3. The encryption method of Claim 1, wherein

the public key vector is obtained by a modulo transformation of a base-product vector.

4. The encryption method of Claim 1, wherein:

the components of the plaintext vector and the transformation vector are expressed by $(m_1, m_2, ..., m_K)$; the components of the public key vector are obtained by a modulo transformation of the components B_i of a base-product vector $(B_1, B_2, ..., B_K)$ (where $B_i = v_i b_1 b_2 ... b_i$, with random numbers v_i and bases b_i $(1 \leqq i \leqq K)$); and as the bases bi, a normal base satisfying $b_i > m_{i-1}$ is used when the m_{i-1} is a component of the plaintext vector while a reduced base satisfying $b_i \leqq m_{i-1}$ is used when the m_{i-1} is a

component of the transformation vector.

5. An encryption method, comprising the step of:

generating a product-sum type ciphertext using a first vector depending on a plaintext and a second vector having components obtained by a modulo transformation of base products; wherein

the first vector is composed of: a plaintext vector obtained by dividing a plaintext to be encrypted; and a transformation vector obtained by a transformation of the plaintext vector using a predetermined function; and wherein the base product is obtained by both normal bases satisfying $b_i > m_{i-1}$ (b_i is a base in the base product, m_{i-1} is a component of the first vector, i is an element of a subset S of a universal set U = {2,3, ..., K}, and K is the number of components of the first and second vector) and reduced bases satisfying $b_j \leqq m_{j-1}$ (b_j is a base in the base product, m_{j-1} is a component of the first vector, and j is an element of a complementary set of the subset S).

6. A decryption method for decrypting a ciphertext generated by the encryption method of Claim 1, wherein the transformation vector is decrypted depending on decrypted components of the plaintext vector.

7. A decryption method for decrypting a ciphertext generated by the encryption method of Claim 2, wherein the transformation vector is decrypted depending on decrypted components of the plaintext vector.

8. A decryption method for decrypting a ciphertext generated

by the encryption method of Claim 3, wherein the transformation vector is decrypted depending on decrypted components of the plaintext vector.

9. A decryption method for decrypting a ciphertext generated by the encryption method of Claim 4, wherein the transformation vector is decrypted depending on decrypted components of the plaintext vector.

10. A decryption method for decrypting a ciphertext generated by the encryption method of Claim 4, wherein a reduced-base part is decrypted depending on a decrypted normal-base part.

11. A decryption method for decrypting a ciphertext generated by the encryption method of Claim 5, wherein a reduced-base part is decrypted depending on a decrypted normal-base part.

12. A cryptographic communication system for communicating information by a ciphertext between entities, comprising:

an encryptor for generating a ciphertext from a plaintext in accordance with the encryption method of Claim 1;

a communication channel for transmitting the generated ciphertext from one entity to another entity; and

a decryptor for decrypting the transmitted ciphertext into a plaintext.

13. A cryptographic communication system for

communicating information by a ciphertext between entities, comprising:

an encryptor for generating a ciphertext from a plaintext in accordance with the encryption method of Claim 2;

a communication channel for transmitting the generated ciphertext from one entity to another entity; and

a decryptor for decrypting the transmitted ciphertext into a plaintext.

14. A cryptographic communication system for communicating information by a ciphertext between entities, comprising:

an encryptor for generating a ciphertext from a plaintext in accordance with the encryption method of Claim 3;

a communication channel for transmitting the generated ciphertext from one entity to another entity; and

a decryptor for decrypting the transmitted ciphertext into a plaintext.

15. A cryptographic communication system for communicating information by a ciphertext between entities, comprising:

an encryptor for generating a ciphertext from a plaintext in accordance with the encryption method of Claim 4;

a communication channel for transmitting the generated ciphertext from one entity to another entity; and

a decryptor for decrypting the transmitted ciphertext into a

plaintext.

16. A cryptographic communication system for communicating information by a ciphertext between entities, comprising:

an encryptor for generating a ciphertext from a plaintext in accordance with the encryption method of Claim 5;

a communication channel for transmitting the generated ciphertext from one entity to another entity; and

a decryptor for decrypting the transmitted ciphertext into a plaintext.

17. An encryption device for generating a product-sum type ciphertext from a plaintext, comprising a controller capable of performing the operations of:

(i) dividing a plaintext to be encrypted thereby to obtain a plaintext vector;

(ii) applying a predetermined transformation on the plaintext vector thereby to generate a transformation vector; and

(iii) generating a ciphertext by a product-sum operation between the components of a public key vector and the components of the plaintext vector and the transformation vector.

18. A computer memory product having computer readable program code means for causing a computer to generate a product-sum type ciphertext from a plaintext, said computer readable program code means comprising:

program code means for causing the computer to divide a

plaintext to be encrypted thereby to obtain a plaintext vector;

program code means for causing the computer to apply a predetermined transformation on the plaintext vector thereby to generate a transformation vector; and

program code means for causing the computer to generate a ciphertext by a product-sum operation between the components of a public key vector and the components of the plaintext vector and the transformation vector.

19. A computer data signal embodied in a carrier wave for transmitting a program, the program being configured to cause a computer to generate a product-sum type ciphertext from a plaintext, comprising:

a code segment for causing the computer to divide a plaintext to be encrypted thereby to obtain a plaintext vector;

a code segment for causing the computer to apply a predetermined transformation on the plaintext vector thereby to generate a transformation vector; and

a code segment for causing the computer to generate a ciphertext by a product-sum operation between the components of a public key vector and the components of the plaintext vector and the transformation vector.